(19) JAPANESE PATENT OFFICE

(3)

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **62205580 A**

(43) Date of publication of application: **10.09.87**

(51) Int. Cl **G11B 20/10**
G11B 7/00

(21) Application number: **61046137**

(22) Date of filing: **05.03.86**

(71) Applicant: **HITACHI LTD**

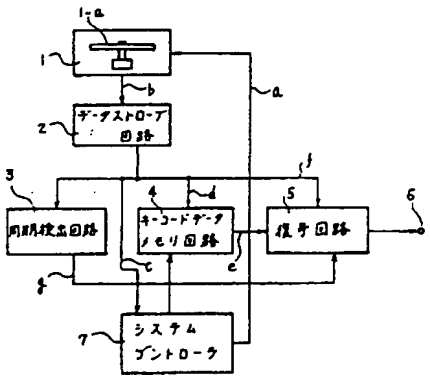
(72) Inventor: **NISHIDA MASAMI**
TAKEUCHI TAKASHI

(54) **DISK AND DATA PROTECTION SYSTEM USING SAME**

(57) Abstract:

PURPOSE: To efficiently supply data and a program at low cost by applying different encipherment to the plural data, and recording a key code for decoding the data required by an user on a disk.

CONSTITUTION: The encipherment capable of decoding by the different key codes by 1:1 is performed to the plural data recorded on the optical disk, cutting is applied to a master disk to duplicate the optical disk. At the time of reading, a system controller 7 reads the key code and stores in a key code memory circuit 4. The required data read from the optical disk 1 recovers the original data by detecting a synchronizing signal and decoding the cipher in a synchronization detecting circuit 3 and decoding circuit 5 through a data strobing circuit 2. When the key code is different from the original one and is not recorded in a position corresponding to the disk, the reading cannot be performed. Thereby, the data or the program of a small capacity can be recorded on the optical disk with large capacity and the data and the program can be supplied efficiently at low cost.



UNEXAMINED PATENT PUBLICATION No. SHO-62-205580

Laid-open date: Sept. 10, 1987

Title of the Invention: Disk and data protection system using the disk

Application No. SHO-61-46137

Application date: March 5, 1986

Inventor: Masami Nishida
c/o Domestic Electrical Appliances Research Institute, Hitachi, Ltd.
No. 292, Yoshida-cho, Tozuka-ku, Yokohama

Inventor: Takashi Takeuchi
c/o Domestic Electrical Appliances Research Institute, Hitachi, Ltd.
No. 292, Yoshida-cho, Tozuka-ku, Yokohama

Applicant: Hitachi, Ltd.
No. 6, Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo

Agent: Katsuo Ogawa, patent attorney, one other

SPECIFICATION

1. Title of the Invention

Disk and data protection system using the disk

2. Scope of Claim for a Patent

(1) A disk for recording a plurality of data differently encrypted, characterized in that a key code data for decrypting the data encrypted as required by the user is recorded in an additionally writable portion, while the key code data for the data not required is not recorded in the additionally writable portion.

(2) A disk as set forth in claim 1, characterized in that said disk is an optical disk.

(3) A disk as set forth in claim 2, characterized in that a disk for recording a plurality of data differently encrypted is used as a master disk, for duplicating the same.

(4) A data protection system for a disk, characterized in that at the time of reproduction, the key code data recorded in the additionally writable portion of the disk is read, so that only those key code data required by the user are decrypted, while the data not required by the user cannot

be decrypted.

Detailed Description of the Invention

[Applicable Field of the invention]

The present invention relates to a disk and a data protection system using the disk, or in particular to a disk and a data protection system for the disk, in which a specific data recorded in the disk can be supplied to the user inexpensively while the other data is protected from being read out.

[Background of the Invention]

In the prior art, an optical disk for supplying a large capacity of data and programs to the user is known in which data and programs of as large as 550 megabytes can be read utilizing a read-only optical disk (compact disk) used for music reproduction ("Compact Disk Used as a Data File Memory", Nikkei Electronics, March 12, 1984).

For a data or a program of a small capacity, however, the production of a single disk for, for example, data of several Kbytes reduces the utilization efficiency of the disk considerably. It is possible to produce a single disk by combining a plurality of data and programs of such small capacity. The chance is slim, however, that all the data are required for each of multiplicity of unspecified users, and supplying data and programs of small capacity to the user in this form leads to the disadvantage of an increased disk cost.

[Object of the Invention]

The object of the present invention is to provide a disk for recording data by a novel method and a data protection system, in which data and programs of small capacity can be supplied to users inexpensively.

[Summary of the Invention]

According to this invention, there is provided a disk for recording a plurality of differently encrypted data, the disk having an additionally writable portion for recording a key code for decrypting the data as required by the user, on the one hand, and a data protection system for decrypting

only the data required by the user by use of the key code recorded in the additionally writable portion of the disk and for prohibiting a decryption of the other data, on the other hand.

[Embodiments of the Invention]

An embodiment of the present invention will be explained below with reference to the drawings.

First, the configuration and the operation of an encryption circuit for recording data in an optical disk will be explained with reference to Fig. 2.

In the encryption circuit of Fig. 2, numerals 8a to 8p designate shift registers, numerals 9a, 9b, 12 EOR (exclusive OR) gates, numeral 10 a key code data input terminal, numeral 11 a data input terminal, and numeral 13 an encryption or decryption data output terminal.

This circuit is an encryption circuit having a M series data generating circuit configured of the shift registers 8 and the EOR gates 9a, 9b, using a generating polynomial G(x),

$G(x) = x^{16} + x^{12} + x^5 + 1$

In recording data, a key code data is assigned to each data to be recorded, and the key code data is input to the shift registers 8 through the key code data input terminal 10. In this case, the key code data is expressed in 16 bits.

Then, when serial data are input from the data input terminal 11, the key code data preset in the shift registers 8 are shifted by the same clock as that for sending the data, and the data constituting a random pattern is output during 2^{16} clocks from the last stage p of the shift registers 8.

The data and the random data are added through the EOR gate 12 thereby to encrypt the data, which is output from the output terminal 13.

The data are assumed to be divided into small blocks and managed by sector on the optical disk as on the magnetic disk. The data only in one division block is encrypted in the manner described above. After encryption, the data with a sync signal or a control signal added to the front of the block is recorded in the optical disk.

At the same time, indexes are recorded without encrypting the same which indicate the tracks and sectors of the optical disk where the data and the key code data are recorded. These are recorded in the master disk for producing the optical disk. After recording by encrypting a plurality of data and programs corresponding to respective key code data, optical disks are duplicated using a stamper from the master disk. In this way, the optical disks can be mass produced.

In the process, an additionally writable portion is also formed. The key code data is recorded in the additionally writable portion in the same manner as the index is recorded previously. The additionally written key code data (2-byte data in this embodiment) is only key code data corresponding to the data used by the user of a given optical disk.

By doing so, in the case where data and programs are copied in magnetic disks and supplied to the users, for example, the need is eliminated to use many copiers or to copy all the data and programs by consuming a long time, and the additional write operation takes a shorter time.

Now, the case in which the user of the optical disk reads the data recorded in the optical disk will be explained with reference to Fig. 1. Fig. 1 is a block diagram showing an optical disk reproduction device.

In the drawing, numeral 1 designates an optical disk drive, numeral 1-a an optical disk in which data are recorded, numeral 2 a data strobe circuit for converting the analog signal read by the laser from the optical disk into a digital signal, numeral 3 a sync signal detection circuit for detecting the sync signal located at the head of the data block, numeral 4 a key code data memory circuit for holding by reading from the disk the key code data used for decryption of the data read, numeral 5 a decryption circuit for decrypting the encrypted data, numeral 6 an output terminal of the decrypted data, and numeral 7 a system controller for controlling the whole of the optical disk device.

First, a control signal a is sent from the system controller 7 to the drive 1, and the signal b read from the optical disk is converted into a digital signal through the data strobe circuit 2. After that, the signal c representing the track and sector address having recorded therein the index information including the file name, the track and sector address of the data and programs recorded in the disk, and the key code data required for decrypting the data and programs is sent to the system controller 7.

Then, an attempt of the user to read the required data or program file causes the system controller 7 to read the key code data that has been used for encrypting the data or the program to be read. In Fig. 1, the key code data d converted into a digital signal and output from the data strobe circuit 2 is input and stored in the key code memory circuit 4.

After that, the intended data or program is read out. These data and programs are segmented into small blocks at the head of each of which a sync signal is added.

The same circuit as the encryption circuit shown in Fig. 2 is used as the circuit 5 for decrypting the encrypted data.

Specifically, the output e of the key code data memory circuit 4 of Fig. 1 is connected to the key code data input terminal 10 of Fig. 2, and the output f of the data strobe circuit 2 of Fig. 1 to the data input terminal 11 of Fig. 2. The data output terminal 6 of Fig. 1 is identical to the data output terminal 13 of Fig. 2.

The intended data read from the optical disk and digitized in the data strobe circuit 2 is input to the sync signal detection circuit 3 and the decryption circuit 5. The sync signal at the head of each small block is detected by the sync signal detection circuit 3. The detection signal g output from this circuit is sent to the decryption circuit 5, so that the key code data e output from the key code data memory circuit 4 is loaded in the shift registers 8 of Fig. 2. As a result, the initial value of the M series data is set.

Then, the encrypted data following the sync signal is input to the data input terminal 11 of the decryption circuit 5. At the same time, the shift registers 8 of the decryption circuit 5 perform the shift operation with the same clock as the data are sent serially. As a result, the encrypted data are added, through the EOR gate 12, to the same M series random data as those used for encryption and restored to the original data.

Specifically, let the original data bits be D, the pattern of the M series be m, and the pattern recorded in the optical disk be D'. Then, the pattern D' can be expressed as follows:

$$D' = D(+)m$$

where (+) is addition in EOR

At the time of decryption, the M series data added to the read data is synchronized by the sync signal to obtain the same data as that at the time of encryption. Then, the decrypted data can be expressed as follows:

$$D'(+)m = (D(+)m)(+)m = D$$

If the key code data is different from the original one, such data is not decrypted since the M series data added to the data for encryption is different from the M series data for decryption.

Further, in the case where the key code data is not recorded in a corresponding area in the optical disk, all of the shift registers 8 are set to "1" to inhibit decryption. Thus, the data in the optical disk is protected by prohibiting the reading thereof in the case where the key code data is different or not recorded.

Instead of the encryption circuit and the decryption circuit utilizing the M series generating circuit according to this embodiment, any type of circuit may be employed which can perform the encryption and decryption operations corresponding to the key code data.

As described above, according to this embodiment, a plurality of data recorded in the optical disk are first encrypted with individually different key codes for

decryption, which data are cut in the master disk from which optical disks are duplicated.

In the case where an optical disk is supplied to a data user, a key code data for decrypting the encrypted data required for the user is recorded in an additionally writable portion of the optical disk, so that the user can read only the required data, while the key codes corresponding to the other unrequired data are not written and therefore cannot be read by the user.

As a result, a multiplicity of data and programs of small capacity can be recorded in an optical disk of large capacity. It is thus not necessary to produce the disk for each data, and the data can be protected. Thus, a great amount of data and programs can be supplied to the users at low cost.

[Effects of the Invention]

According to this invention, a plurality of data and programs of small capacity can be recorded in a single disk of large capacity, and the data and programs to be read can be specified for each user, while the unrequired data and programs can be protected by preventing them from being read. As a result, only a single disk is cut and duplicated for a plurality of data and programs, thereby making it possible to supply data and programs efficiently and inexpensively.

4. Brief Description of the Drawings

Fig. 1 is a block diagram showing an optical disk reproduction device according to an embodiment of the present invention, and Fig. 2 is a circuit diagram showing an example of the circuit for encrypting or decrypting the data.

1...Optical disk drive, 3...Sync signal detection circuit, 4...Key code data memory circuit, 5...Decryption circuit, 6...Data output terminal, 8...Shift registers, 9a, 9b, 12...EOR gates, 10...Key code data input terminal, 11...Data input terminal, 12...Data output terminal.

するM系列データを暗号化した時と同じデータとなるように同期信号により同期させると、復号されたデータは次のように表わされる。

$\hat{D} \oplus m = (D \oplus m) \oplus m = D$

また、このときキーコードデータが本来のものと異なつていると、データに加算されるM系列データが暗号化時と復号化時に異なるため、データとしては復号されない。

さらに、キーコードデータが光ディスクの対応するところに記録されていない場合には、シフトレジスタ8を全て"1"にセットして復号がされないようにして、キーコードデータの異なるもの、及び記録されていない場合に、光ディスクからのデータの読み出しができないよう保護する。

なお、この実施例ではM系列発生回路を利用した暗号化，復号化回路を構成しているが、キーコードデータに対応した暗号化，復号化できる回路であればどのような方式のものでもよい。

以上のように、本実施例によれば、まず光ディスクに記録する複数のデータに、それぞれ1対1の異なつたキーコードで復号できる暗号化を行なつてそのデータをマスタディスクにカッティングし、そのマスタディスクから光ディスクを複製して作る。

光ディスクをデータ利用者に供給する場合にはその利用者が必要な暗号化されたデータを復号するキーコードデータを光ディスクの追記可能な部分に記録しておき、必要なデータだけを利用者が読めるようにし、その他の不必要なデータは対応したキーコードを書かないようにして利用者には読めないようにする。

これにより、小容量のデータやプログラムが大容量の光ディスクに多数記録でき、データごとにディスクを作る必要がなく、データも保護できるため、データやプログラムを利用者に大量に、また安価に供給することができる。

〔発明の効果〕

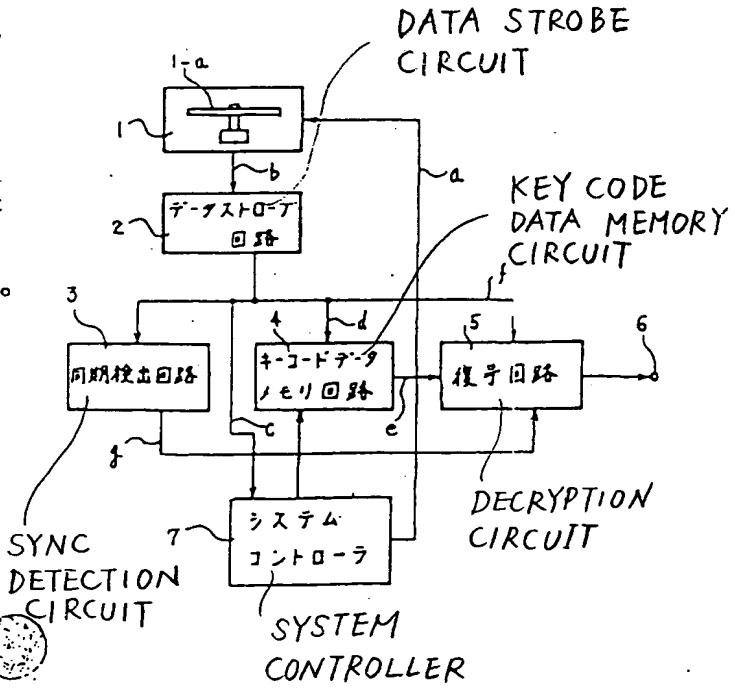
本発明によれば、複数の小容量データ及びプログラムを大容量ディスク1枚に記録することができ、利用者に応じて読み出せるデータ及びプログラムの限定が行なえ、必要でないデータ及びプログラムに対しては読み出せないように保護することができる。このため、複数のデータ及びプログラムに対して1枚のディスクをカッティング、複製すればよく、データ及びプログラムの供給を効率よく安価に行なえる。

4 図面の簡単な説明

第1図は本発明の一実施例の光ディスク再生装置のブロック図、第2図はデータを暗号化または復号化する回路の一例を示す回路図である。

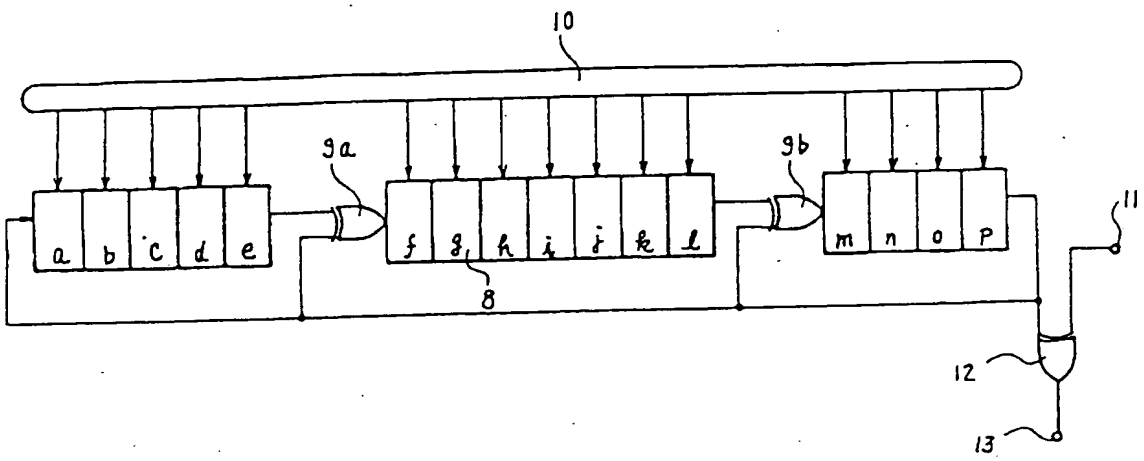
1…光ディスクドライブ　3…同期信号検出回路　4…キーコードデータメモリ回路　5…復号回路　6…データ出力端子　8…シフトレジスタ　9a，9b，12…EORゲート　10…キーコードデータ入力端子　11…データ入力端子　12…データ出力端子

Fig. 1
第1図



代理人弁理士　小　川　勝　男

Fig. 2
第2図



⑲日本国特許庁(JP)　⑪特許出願公開　(3)

⑫公開特許公報(A)　昭62-205580

⑤1Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)9月10日
G 11 B 20/10		R-6733-5D	
7/00		A-7520-5D	

審査請求　未請求　発明の数 2　(全5頁)

⑤4発明の名称　ディスクおよびそれを用いたデータ保護方式

㉑特　願　昭61-46137
㉒出　願　昭61(1986)3月5日

㉗発明者　西田　正己　横浜市戸塚区吉田町292番地　株式会社日立製作所家電研究所内
㉗発明者　竹内　崇　横浜市戸塚区吉田町292番地　株式会社日立製作所家電研究所内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1　発明の名称　ディスクおよびそれを用いたデータ保護方式

2　特許請求の範囲

(1)　それぞれ異なつた暗号化が施された複数のデータを記録し、利用者の必要に応じて、その必要な暗号化されたデータを復号するためのキーコードデータを、追記可能部分に記録、必要でないデータに対するキーコードデータは該追記可能部分に記録しないようにしたことを特徴とするディスク。

(2)　前記ディスクが光ディスクであることを特徴とする前記特許請求の範囲第1項記載のディスク。

(3)　異なる暗号化が施された複数のデータを記録するディスクをマスタディスクとして、複製されたことを特徴とする前記特許請求の範囲第2項記載のディスク。

(4)　再生時に、ディスクの追記可能部分に記録されたキーコードデータを読み出し、該キーコードデータで利用者が必要とするデータのみを復号し、利用者が必要としないデータは復号できないようにしたことを特徴とするディスクのデータ保護方式。

3　発明の詳細な説明

〔発明の利用分野〕

本発明はディスクおよびそれを用いたデータ保護方式に係り、特にディスクに記録された特定のデータをユーザに安価に供給し、他のデータは読み出しできないように保護するのに好適なディスクおよびそのデータ保護方式に関する。

〔発明の背景〕

従来、大容量のデータやプログラムをその利用者に供給するものとして、音楽再生専用光ディスク(コンパクトディスク)を応用し、550メガバイトものデータやプログラムの読み出しを可能にした光ディスクが知られている(日経エレクトロニクス、1984、3.12、「コンパクト・ディスクをデータ・ファイル・メモリに使う」)。

しかし、小容量のデータやプログラムに対し

ては、例えば数キロバイトのデータに対して1枚のディスクを作ると、ディスクの利用効率が大変悪い。そこで、そのような小容量のデータやプログラムを複数まとめて1枚のディスクを作ることも可能ではあるが、不特定多数の利用者としては全てのデータが必要となる可能性は少なく、このような方法で小容量のデータやプログラムを利用者に提供すると、ディスク価格の上昇につながるという欠点があつた。

〔発明の目的〕

本発明の目的は、新規な方法でデータが記録されたディスクおよびデータ保護方式を提供することにより、小容量のデータやプログラムの利用者に対して、これらのデータやプログラムを安価に供給することができるようにすることにある。

〔発明の概要〕

本発明は、複数のデータにそれぞれ異なつた暗号化を施して記録し、かつ追記可能部分に利用者が必要とするデータを復号するためのキーコードを記録したディスクを提供した点、および該ディスクの追記可能部分に記録されたキーコードを用いて利用者が必要とするデータのみを復号し、他のデータは復号できないデータ保護方式を提供した点に特徴がある。

〔発明の実施例〕

以下に、本発明の一実施例を図面を用いて説明する。

まず、光ディスクにデータを記録する場合の暗号化回路の構成および動作について第2図を用いて説明する。

第2図の暗号化回路において、8のa～pはシフトレジスタ，9a，9bおよび12はEORゲート（排他的論理和ゲート），10はキーコードデータ入力端子，11はデータ入力端子，13は暗号化または復号化データ出力端子である。

この回路は、シフトレジスタ8とEORゲート9a，9bとで構成される生成多項式G(x)が

$$G(x) = x^{16} + x^{12} + x^5 + 1$$

のM系列データ生成回路である回路を有する暗号化回路である。

データを記録する場合、記録するデータ1つに対し、1つのキーコードデータを割り当て、そのキーコードデータをキーコードデータ入力端子10からシフトレジスタ8に入力する。ここではキーコードデータは16ビットで表わされる。

次にシリアルデータがデータ入力端子11から入力されると、データが送られるクロックと同じクロックによりシフトレジスタ8のプリセットされたキーコードデータがシフトされ、シフトレジスタ8の最終段pから2^{16}のクロックの間でランダムパターンとなるデータが出力される。

そこで、EORゲート12によりデータとランダムデータとがEOR加算されることによりデータの暗号化がなされ、出力端子13より出力される。

なお、データは光ディスク上では磁気ディスク同様小さなブロックに分割してセクタ管理されるものとし、分割された1ブロックのデータに対してのみ上記の暗号化が行なわれ、暗号化された後にそのブロックの前に同期信号や制御信号が付加されて光ディスクに記録される。

また、その光ディスクにデータ及びキーコードデータの記録されたトラック，セクタを示すインデックスを暗号化せず記録しておく。これらは光ディスクを作るときのマスタディスクに記録されるものであり、複数のデータやプログラムがそれぞれのキーコードデータに対応した暗号化がなされて記録された後、このマスタディスクからスタンパを用いて複製して光ディスクを作ることにより、光ディスクの大量生産ができる。

このとき追記可能な部分も作つておく。この追記可能な部分には先にインデックスとして記録された通りに、キーコードデータを追記する。このとき追記するキーコードデータ（本実施例では、2バイトのデータ）は光ディスクの利用者に対応して利用するデータに対応したキーコードデータのみ追記する。

このようにすれば、磁気ディスクにデータやプログラムをコピーして利用者に供給する場合のように、多くのコピー装置を用いたり、多大な時間をかけてデータやプログラム全てをコピーする必要性がなく、追記する時間も短かくてすむ。

次に光ディスクの利用者が光ディスクに記録されたデータを読む場合について第1図を用いて説明する。第1図は光ディスク再生装置のブロック図を示す。

図において、1は光ディスクドライブ，1－aはデータが記録されている光ディスク，2は光ディスクからレーザにより読み出されたアナログ信号をディジタル信号に変換するためのデータストローブ回路，3はデータブロックの先頭にある同期信号を検出するための同期信号検出回路，4は読み出すデータの復号化に用いるキーコードデータをディスクから読み出して保持しておくキーコードデータメモリ回路，5は暗号化されたデータの復号を行なう復号回路，6は復号化されたデータの出力端子，7は光ディスク装置全体をコントロールするシステムコントローラである。

まず、システムコントローラ7からドライブ1に制御信号aが送られ、光ディスクから読み出された信号bはデータストローブ回路2を通してディジタル信号に変換された後、ディスクに記録されているデータ及びプログラムのファイル名，トラック及びセクタ番地等のインデックス情報各データ及びプログラムの復号に必要なキーコードデータの記録されているトラックおよびセクタ番地の信号cがシステムコントローラ7に送られる。

次に利用者が必要なデータまたはプログラムファイルの読み出しを行なおうとすると、システムコントローラ7は、読み出されるべきデータまたはプログラムを暗号化した時に用いたキーコードデータの読み出しを行なう。第1図ではデータストローブ回路2から出力された、ディジタル信号に変換されたキーコードデータdが、キーコードメモリ回路4に入力され記憶される。

この後に目的のデータまたはプログラムが読み出されるが、これらは小さなブロックに分割されその先頭に同期信号が付加されている。

この暗号化されたデータの復号を行なう回路5としては第2図の暗号化回路と同じ回路を用いる。

つまり第1図のキーコードデータメモリ回路4の出力eは第2図のキーコードデータ入力端子10に、第1図のデータストローブ回路2の出力fが第2図のデータ入力端子11につながる。また、第1図のデータ出力端子6と、第2図のデータ出力端子13とは同じものである。

光ディスクから読み出され、データストローブ回路2でディジタル化された目的のデータは、同期信号検出回路3及び復号回路5に入力され、まず各小さなブロックの先頭にある同期信号が、同期信号検出回路3により検出される。これから出力される検出信号gは、復号回路5に送られ、第2図のシフトレジスタ8にキーコードデータメモリ回路4から出力されるキーコードデータeをロードする。これによりM系列データの初期値を設定する。

次に、同期信号の後につづく暗号化されたデータは復号回路5のデータ入力端子11に入力される。これとともに、データがシリアルで送られるのと同じクロックで復号回路5のシフトレジスタ8がシフト動作を行なう。これによつて、前記暗号化されたデータは暗号化を行なつたときと同じM系列のランダムデータとEORゲート12によりEOR加算され、元のデータに復号される。

つまり、元のデータビットをDとし、M系列のパターンをm、光ディスクに記録されるパターンを$\hat{D}$とすると、パターン$\hat{D}$は次のように表わされる。

$\hat{D} = D \oplus m$

$\oplus$：EOR加算

また、復号時には、読み出したデータに加算

するM系列データを暗号化した時と同じデータとなるように同期信号により同期させると、復号されたデータは次のように表わされる。

$$(D \oplus m) \oplus m = D$$

また、このときキーコードデータが本来のものと異なつていると、データに加算されるM系列データが暗号化時と復号化時に異なるため、データとしては復号されない。

さらに、キーコードデータが光ディスクの対応するところに記録されていない場合には、シフトレジスタ8を全て"1"にセットして復号がされないようにして、キーコードデータの異なるもの、及び記録されていない場合に、光ディスクからのデータの読み出しができないよう保護する。

なお、この実施例ではM系列発生回路を利用した暗号化，復号化回路を構成しているが、キーコードデータに対応した暗号化，復号化できる回路であればどのような方式のものでもよい。

以上のように、本実施例によれば、まず光ディスクに記録する複数のデータに、それぞれ1対1の異なつたキーコードで復号できる暗号化を行なつてそのデータをマスタディスクにカッティングし、そのマスタディスクから光ディスクを複製して作る。

光ディスクをデータ利用者に供給する場合にはその利用者が必要な暗号化されたデータを復号するキーコードデータを光ディスクの追記可能な部分に記録しておき、必要なデータだけを利用者が読めるようにし、その他の不必要なデータは対応したキーコードを書かないようにして利用者には読めないようにする。

これにより、小容量のデータやプログラムが大容量の光ディスクに多数記録でき、データごとにディスクを作る必要がなく、データも保護できるため、データやプログラムを利用者に大量に、また安価に供給することができる。

〔発明の効果〕

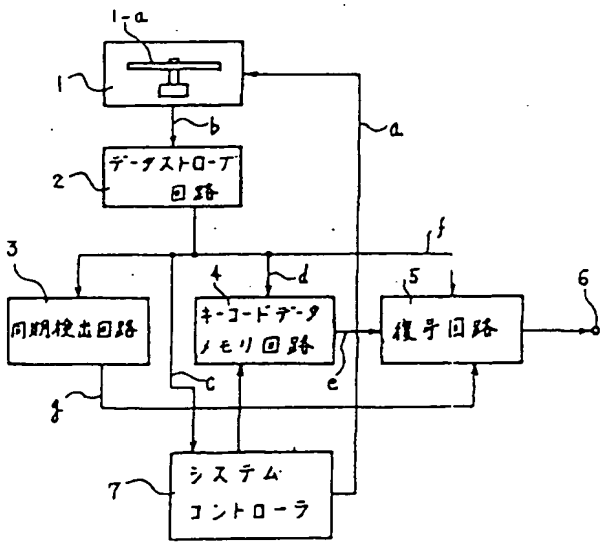
本発明によれば、複数の小容量データ及びプログラムを大容量ディスク1枚に記録することができ、利用者に応じて読み出せるデータ及びプログラムの限定が行なえ、必要でないデータ及びプログラムに対しては読み出せないように保護することができる。このため、複数のデータ及びプログラムに対して1枚のディスクをカッティング、複製すればよく、データ及びプログラムの供給を効率よく安価に行なえる。

4 図面の簡単な説明

第1図は本発明の一実施例の光ディスク再生装置のブロック図、第2図はデータを暗号化または復号化する回路の一例を示す回路図である。

1…光ディスクドライブ　3…同期信号検出回路　4…キーコードデータメモリ回路　5…復号回路　6…データ出力端子　8…シフトレジスタ　9a，9b，12…EORゲート　10…キーコードデータ入力端子　11…データ入力端子　12…データ出力端子

第1図



代理人弁理士　小　川　勝　男

第2図